#4

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
MARINET ET AL.

Serial No. **09/995,258**

Confirmation No. **1339**

Filing Date: **NOVEMBER 27, 2001**

For: **RANDOM SIGNAL GENERATOR**

COPY OF PAPERS ORIGINALLY FILED

TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Director, U.S. Patent and Trademark Office
Washington, D.C. 20231

Sir:

Transmitted herewith is a certified copy of the priority French Application No. 00 15309.

Respectfully submitted,

CHRISTOPHER F. REGAN
Reg. No. 34,906
Allen, Dyer, Doppelt, Milbrath
& Gilchrist, P.A.
255 S. Orange Avenue, Suite 1401
Post Office Box 3791
Orlando, Florida 32802
Telephone: 407/841-2330
Fax: 407/841-2343
Attorney for Applicant

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: DIRECTOR, U.S. PATENT AND TRADEMARK OFFICE, WASHINGTON, D.C. 20231, on this 30th day of January, 2002.

Dawn Kimler

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 07 NOV. 2001

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

CERTIFIED COPY OF PRIORITY DOCUMENT

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (1) 53 04 53 04
Télécopie : 33 (1) 42 93 59 30
www.inpi.fr

ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

cerfa N° 11354*01

Code de la propriété intellectuelle - Livre VI

REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 W / 260899

Réservé à l'INPI

REMISE DES PIÈCES
DATE 28 NOV 2000
LIEU 13 INPI MARSEILLE

N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0015309

DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 28 NOV. 2000

Vos références pour ce dossier *(facultatif)* 100115 FR

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

OMNIPAT
MARCHAND André
24 Place des Martyrs de la Résistance
13100 AIX EN PROVENCE

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE	**Cochez l'une des 4 cases suivantes**
Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date / /
ou demande de certificat d'utilité initiale	N° Date / /
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date / /

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

GENERATEUR DE SIGNAL ALEATOIRE

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE	
	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

5 DEMANDEUR		☐ **S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»**
Nom ou dénomination sociale		STMICROELECTRONICS
Prénoms		
Forme juridique		SOCIETE ANONYME
N° SIREN		3 4 1 4 5 9 3 8 6
Code APE-NAF		3 2 1 B
Adresse	Rue	7, Avenue Galliéni
	Code postal et ville	94250 GENTILLY CEDEX
Pays		FRANCE
Nationalité		FRANCE
N° de téléphone *(facultatif)*		
N° de télécopie *(facultatif)*		
Adresse électronique *(facultatif)*		

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE 2/2

Réservé à l'INPI

REMISE DES PIÈCES
DATE 28 NOV 2000
LIEU 13 INPI MARSEILLE

N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0015309

DB 540 W /260899

Vos références pour ce dossier : *(facultatif)*		100115 FR
6 MANDATAIRE		
Nom		MARCHAND
Prénom		André
Cabinet ou Société		OMNIPAT
N °de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	24 Place des Martyrs de la Résistance
	Code postal et ville	13100 AIX EN PROVENCE
N° de téléphone *(facultatif)*		04.42.99.06.60.
N° de télécopie *(facultatif)*		04.42.99.06.69.
Adresse électronique *(facultatif)*		
7 INVENTEUR (S)		
Les inventeurs sont les demandeurs		☐ Oui ☒ Non **Dans ce cas fournir une désignation d'inventeur(s) séparée**
8 RAPPORT DE RECHERCHE		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance		**Paiement en trois versements, uniquement pour les personnes physiques** ☐ Oui ☒ Non
9 RÉDUCTION DU TAUX DES REDEVANCES		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Requise antérieurement à ce dépôt *(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence)*
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(Nom et qualité du signataire)
MARCHAND André - CPI N° 95 0303
OMNIPAT

VISA DE LA PRÉFECTURE OU DE L'INPI

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11235*02

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

DÉSIGNATION D'INVENTEUR(S) Page N° 1 / 1
(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire. DB 113 W /260899

28 NOV 2000
13 INPI MARSEILLE

Vos références pour ce dossier *(facultatif)*	100115FR
N° D'ENREGISTREMENT NATIONAL	0015309

TITRE DE L'INVENTION (200 caractères ou espaces maximum)
GENERATEUR DE SIGNAL ALEATOIRE

LE(S) DEMANDEUR(S) :

MARCHAND André
OMNIPAT
24, Place des Martyrs de la Résistance
13100 AIX EN PROVENCE

DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).

Nom		MALHERBE
Prénoms		Alexandre
Adresse	Rue	C/O OMNIPAT 24 Place des Martyrs de la Résistance
	Code postal et ville	13100 AIX EN PROVENCE
Société d'appartenance *(facultatif)*		
Nom		MARINET
Prénoms		Fabrice
Adresse	Rue	C/O OMNIPAT 24 Place des Martyrs de la Résistance
	Code postal et ville	13100 AIX EN PROVENCE
Société d'appartenance *(facultatif)*		
Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance *(facultatif)*		

DATE ET SIGNATURE(S)
DU (DES) DEMANDEUR(S)
OU DU MANDATAIRE
(Nom et qualité du signataire)
Aix en Provence, le 27 novembre 2000
MARCHAND André - CPI N° 95 0303
OMNIPAT

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

GENERATEUR DE SIGNAL ALEATOIRE

La présente invention concerne un procédé et un dispositif pour la génération d'un signal aléatoire.

La présente invention s'applique notamment, mais non exclusivement, à la réalisation d'un générateur de signal binaire aléatoire pour carte à puce.

Un générateur de signal binaire aléatoire permet par exemple à une carte à puce, au cours d'une procédure d'authentification d'un terminal, d'envoyer au terminal une séquence binaire aléatoire comprenant par exemple 16 ou 32 bits. La carte et le terminal appliquent à cette séquence une fonction d'authentification à clé secrète. Le terminal transmet ensuite à la carte le résultat obtenu, et la carte compare le résultat qu'elle a calculé avec celui qu'elle a reçu du terminal. Si les deux résultats sont identiques, le terminal est présumé authentique et la carte accepte la transaction demandée.

On connaît dans l'art antérieur des générateurs d'aléas se présentant sous la forme d'une machine logique comportant un nombre fini d'états internes. Une telle machine logique comprend par exemple des registres à décalage dont certains bits sont renvoyés en entrée de la machine par l'intermédiaire d'une porte OU Exclusif. A partir d'un état interne initial, on active la machine logique au moyen d'un signal d'horloge et l'on extrait de la machine logique, à chaque coup d'horloge, un bit aléatoire.

Toutefois, l'inconvénient de telles machines logiques est qu'elles génèrent des séquences binaires déterministes qui présentent un taux élevé de répétitivité, ainsi qu'un biais statistique de sortie

portant sur la répartition des "1" et des "0". Pour pallier cet inconvénient, il faut prévoir des machines logiques présentant un grand nombre d'états internes (l'idéal étant que la machine présente un nombre infini d'états internes), mais cette solution va à l'encontre des exigences de simplicité, de faible coût et de faible consommation des générateurs aléatoires.

Un générateur de signal aléatoire peut également être réalisé au moyen d'une source de bruit électronique, telle que le bruit d'une diode en avalanche ou d'une diode polarisée, ou encore le bruit thermique dans une résistance. Toutefois, ces sources de bruit sont de très faible amplitude, de sorte qu'il est nécessaire de prévoir un amplificateur à gain élevé, au minimum de 60 dB, impliquant l'utilisation de transistors bipolaires qui présentent une consommation importante. Or, la présence de tels transistors est exclue dans de nombreux circuits intégrés, notamment ceux destinés aux cartes à puce.

Ainsi, un objectif de la présente invention est de prévoir un générateur de signal aléatoire qui ne présente pas les inconvénients des générateurs connus.

Pour atteindre cet objectif, la présente invention se fonde sur la constatation selon laquelle les transistors MOS coudés, présentant un canal en lacets, sont réputés inutilisables lorsque l'on se trouve à la limite de la technologie d'intégration employée, du fait que le courant drain-source dans de tels transistors présente une composante aléatoire de plus en plus importante au fur et à mesure que les dimensions du canal en lacets diminuent. Une idée de la présente invention est de tirer profit de cet inconvénient pour réaliser un générateur de signal aléatoire intégrable dans un circuit intégré, notamment un circuit intégré pour carte à puce.

Ainsi, la présente invention prévoit un générateur de signal aléatoire du type utilisant une source de

bruit électronique, dans lequel la source de bruit électronique comprend un transistor MOS coudé présentant un courant drain-source ayant une composante aléatoire, le générateur comprenant des moyens pour produire un signal binaire aléatoire à partir de la composante aléatoire.

Selon un mode de réalisation, le transistor MOS coudé comprend un canal en forme de S ou en lacets dont les dimensions sont à la limite de la résolution offerte par la technique de fabrication du transistor.

Selon un mode de réalisation, le générateur comprend un transistor de référence auquel sont appliqués une tension de grille et un courant de polarisation identiques à ceux appliqués au transistor coudé, pour extraire la composante aléatoire.

Selon un mode de réalisation, le générateur comprend des moyens pour comparer la composante aléatoire à un courant de détection.

Selon un mode de réalisation, le générateur comprend des moyens pour amplifier la composante aléatoire.

Selon un mode de réalisation, le générateur comprend des moyens pour échantillonner le signal binaire aléatoire, de manière à obtenir un signal numérique aléatoire.

Selon un mode de réalisation, le générateur comprend un circuit logique pour produire des nombres binaires aléatoires à partir du signal numérique aléatoire.

Selon un mode de réalisation, le générateur comprend des moyens pour maintenir automatiquement la tension de grille du transistor coudé dans une plage de valeurs déterminée assurant la délivrance d'un signal de sortie équiprobable.

Selon un mode de réalisation, le générateur comprend plusieurs sources de bruit électronique produisant un courant ayant une composante aléatoire,

chaque source étant couplée respectivement à des moyens pour générer un signal binaire aléatoire à partir de la composante aléatoire produite par la source, le générateur comprenant en outre des moyens pour combiner les signaux binaires aléatoires issus des sources pour produire des nombres binaires aléatoires.

La présente invention concerne également un circuit intégré comprenant un générateur de signal binaire aléatoire selon l'invention, et des moyens pour relier la sortie du générateur à d'autres composants du circuit intégré.

Selon un mode de réalisation, le circuit intégré est agencé sur un support pour former une carte à puce ou tout autre objet électronique portable équivalent.

Selon un mode de réalisation, le circuit intégré comprend une unité de traitement comprenant des moyens pour recevoir un nombre aléatoire produit par le générateur, des moyens pour émettre ce nombre aléatoire à destination d'un terminal extérieur, des moyens pour appliquer à ce nombre aléatoire une fonction d'authentification à clé secrète, des moyens pour comparer le résultat de cette fonction à un résultat fourni par le terminal en réponse à l'émission du nombre aléatoire, et des moyens pour autoriser une transaction avec le terminal si le résultat fourni par le terminal correspond au résultat calculé par l'unité de traitement.

La présente invention concerne également un procédé pour générer un signal aléatoire à partir d'une source de bruit électronique, comprenant les étapes consistant à prévoir un transistor coudé présentant un canal en forme de S ou en lacets dont les dimensions sont choisies à la limite de la résolution offerte par la technique de fabrication du transistor, extraire une composante aléatoire de courant aux bornes d'un transistor MOS coudé, générer un signal binaire en

fonction de la composante aléatoire, et échantillonner le signal binaire.

Selon un mode de réalisation, le procédé comprend des étapes consistant à amplifier la composante aléatoire et lui retrancher une valeur de référence avant de la convertir en un signal binaire.

Selon un mode de réalisation, le procédé comprend une étape d'ajustement de la tension de grille du transistor coudé en fonction du signal binaire aléatoire obtenu à la suite de l'étape d'échantillonnage.

Selon un mode de réalisation, le procédé comprend une étape consistant à générer des nombres binaires à partir du signal binaire.

Ces objets, caractéristiques et avantages ainsi que d'autres de la présente invention seront exposés plus en détail dans la description suivante d'un générateur selon l'invention, faite à titre non limitatif en relation avec les figures jointes parmi lesquelles :

- la figure 1 est le schéma électrique d'un générateur aléatoire selon l'invention,
- la figure 2 est une vue détaillée d'un composant de référence présent dans le générateur de la figure 1,
- la figure 3 est une vue détaillée d'un composant utilisé comme source de bruit dans le générateur de la figure 1,
- la figure 3a représente un détail du composant représenté en figure 3,
- la figure 4 représente des courbes de variation du courant dans le composant de référence et le composant source de bruit en fonction d'une tension appliquée à ces composants,
- la figure 5 représente des courbes de variation du courant en un autre point du générateur aléatoire, en fonction de la tension appliquée aux composants de référence et source de bruit,

- la figure 6 représente sous forme de blocs un exemple d'application d'un générateur de signal aléatoire selon l'invention, et

- la figure 7 représente un générateur aléatoire comprenant plusieurs générateurs selon l'invention.

La figure 1 représente un générateur de signaux binaires aléatoires RGEN 1 selon l'invention. Le générateur comprend un transistor M_c utilisé comme source de bruit électronique, ainsi qu'un transistor de référence M_{ref}. Selon l'invention, le transistor M_c est de type MOS coudé présentant un courant drain-source qui varie d'une manière aléatoire dans une plage déterminée de valeurs, pour une tension de grille donnée. Le transistor de référence M_{ref} présente des caractéristiques analogues à celles du transistor M_c, mais sans composante aléatoire.

Le générateur 1 comprend deux transistors M1, M2 agencés en miroir de courant qui polarisent les deux transistors M_{ref} et M_c en appliquant sur leur drain un même courant I_1. La source du transistor M_c est connectée à la masse tandis que la source du transistor M_{ref} est reliée à la masse par l'intermédiaire d'une résistance R d'équilibrage de la résistance drain-source du transistor M_c. Du fait que le courant drain-source dans le transistor M_c présente une composante aléatoire, le courant au niveau du drain est égal à $I_1+\Delta I$.

La figure 4 représente les courbes de variation 31, 32 en fonction de la tension de grille V_G, des courants drain-source I_{ref} et I_c, respectivement dans les transistors M_{ref} et M_c. Il apparaît que plus la tension V_G augmente, plus la composante aléatoire ΔI (largeur de la zone hachurée 32) du courant I_c augmente.

Le générateur 1 comprend en outre deux transistors M3, M4 également agencés en miroir de courant, la source et la grille du transistor M3 étant connectée au drain du transistor M_c. De cette manière, le transistor M3 mesure la différence de courant $\Delta I=I_c-I_{ref}$ entre les

courants de drain des transistors M_C et M_{ref}, et le courant I_2 à la source du transistor M4 correspond au courant ΔI multiplié par un gain α, de sorte que $I_2 = \alpha \cdot \Delta I$. Le transistor M4 est surdimensionné par rapport au transistor M3, de sorte que le rapport d'amplification ou gain α soit supérieur à 1, par exemple égal à 2.

La figure 5 représente la courbe de variation du courant I_2 en fonction de la tension de grille V_G. Comme le courant I_c comporte une composante aléatoire, le courant I_2 présente également une composante aléatoire représentée par la zone hachurée 35.

La source du transistor M4 est connectée à une source de courant S_s fournissant un courant de détection de référence I_s (représenté sur la figure 5), de manière à obtenir sur la source du transistor M4 un courant égal à I_2-I_s. Ce courant différentiel est appliqué à l'entrée d'une porte inverseuse 2 dont la sortie délivre un signal logique égal à 0 lorsque I_2 est supérieur à I_s et égal à 1 dans le cas contraire. Le signal logique est échantillonné au moyen d'une bascule 4 de type D dont l'entrée D est connectée à la sortie de la porte 2 et dont la sortie Q délivre le signal binaire aléatoire. L'entrée d'horloge CK de la bascule 4 est pilotée par un signal d'horloge Clk de fréquence déterminée, délivré par un oscillateur 3 interne ou externe au générateur.

Pour que le courant I_2 oscille d'une manière aléatoire autour du courant I_s, le signal sur la sortie Q de la bascule 4 est renvoyé sur la grille des transistors M_{ref} et M_C par l'intermédiaire d'un circuit intégrateur permettant d'ajuster automatiquement la tension de grille V_G. De ce fait, la tension de grille V_G se trouve comprise dans une zone délimitée par des valeurs $V_G$min et $V_G$max représentées en figure 5, correspondant à la largeur de la zone hachurée 35.

Le circuit intégrateur comprend ici un transistor PMOS M5 et un transistor NMOS M6. La source du transistor M5 est reliée au drain du transistor M6 par

l'intermédiaire de deux sources de courant S1, S2 en série. Le signal délivré par la sortie Q de la bascule 4 est appliqué sur les grilles des deux transistors M5 et M6 et le nœud de jonction des sources de courant S1, S2 est relié aux grilles des transistors M_C et M_{ref}. La grille des deux transistors M_C et M_{ref} est par ailleurs reliée à la masse par l'intermédiaire d'un condensateur C qui complète les capacités de grille relativement élevées des transistors M_{ref} et M_C pour intégrer la tension de grille V_G en se chargeant et en se déchargeant à courant constant.

Ainsi, lorsque le signal présent sur la sortie Q de la bascule 4 est à 0, le transistor M6 est bloqué et le transistor M5 est passant. La source de courant S1 applique alors un courant au nœud de connexion des grilles des transistors M_{ref}, M_C et de la capacité C.

Si au contraire le niveau logique du signal appliqué à l'entrée du circuit intégrateur est à 1, le transistor M5 est bloqué et le transistor M6 est passant. La source de courant S2 applique alors un courant au nœud de connexion des grilles des transistors M_{ref}, M_C et de la capacité C.

Ainsi, le dispositif intégrateur suit en permanence les variations de courant dans le transistor M_C de manière que la tension de grille V_G reste comprise entre $V_G$min et $V_G$max et que les bits à "1" ou à "0" à la sortie du générateur soient équiprobables.

Les figures 2 et 3 représentent plus en détail les transistors M_{ref} et M_C. Sur la figure 2, le transistor MOS M_{ref} comprend d'une manière classique plusieurs canaux 14 rectilignes et parallèles, formés par implantation de dopant dans un substrat semi-conducteur, l'ensemble de ces canaux étant recouvert par une grille 11 constituée d'une couche mince électriquement isolante, par exemple en polysilicium (silicium polycristallin), cette couche étant recouverte d'une métallisation constituant la connexion de grille. Les extrémités de chaque canal 14

sont munies de zones de contact 13, 19 et sont interconnectées en série par des métallisations 17 représentées en traits interrompus, deux zones de contact 13, 19 extrêmes de la chaîne ainsi réalisée, étant munis de métallisations, respectivement 12, 18, constituant les connexions de drain et de source du transistor. En d'autres termes, le transistor M_{ref} est constitué de plusieurs transistors montés en série avec une grille commune.

Sur la figure 3, le transistor M_c comprend un canal 24 également formé par implantation de dopant dans un substrat semi-conducteur, ce canal présentant une forme en S ou en lacets, avec plusieurs parties parallèles les unes aux autres reliées par des parties coudées sensiblement de même largeur que les parties parallèles. L'ensemble du canal 24 est recouvert par une grille 21 constituée d'une couche mince électriquement isolante, par exemple en polysilicium, cette couche étant recouverte d'une métallisation constituant la connexion de grille. Les deux extrémités du canal comportent des contacts 23, 29 reliés à des métallisations respectives 22, 28 constituant respectivement les connexions de drain et de source du transistor. Le courant drain-source présente une composante aléatoire lorsque les dimensions du canal sont choisies proches du minimum de résolution offert par la technique de fabrication utilisée, voire légèrement inférieures à ce minimum, car l'on obtient alors des imperfections lors du développement du masque d'implantation du canal.

Ainsi, comme cela apparaît sur la vue agrandie de la figure 3a, lorsque le canal présente des dimensions et un pas de repliement des coudes proches de la limite offerte par technologie employée, voire légèrement inférieurs à cette limite, les parties coudées obtenues présentent une forme arrondie 24' à l'intérieur du coude.

Par exemple, avec une technologie d'intégration de 0,35 μm, la largeur des parties parallèles et coudées de la grille est inférieure à 1 μm, de préférence voisine de 0,7 μm, tandis que la distance entre les parties parallèles est de l'ordre de 1,5 μm.

Plus le nombre de coudes d'un tel transistor est élevé, plus la composante aléatoire ΔI du courant drain-source est importante. En contrepartie, le courant drain-source est plus faible et nécessite d'être amplifié avec un gain élevé. Il existe donc un nombre optimum de coudes qui dépend de l'échelle d'intégration du composant, par exemple 10 coudes dans un mode de réalisation testé par la demanderesse.

Le générateur 1 peut être couplé à un circuit logique 5 (figure 1) conçu pour générer à partir des trains de bits en sortie de la bascule 4, des nombres aléatoires d'une longueur en bits prédéfinie (par exemple 8, 16, 32 bits...). Ce circuit peut être un simple convertisseur série/parallèle ou être équipé de moyens permettant de combiner d'une manière plus complexe les bits du signal série appliqué en entrée. Ces moyens de combinaison peuvent par exemple être conçus pour corriger des éventuels défauts statistiques et améliorer le caractère aléatoire des nombres qui sont produits en sortie.

Alternativement, comme représenté sur la figure 7, plusieurs générateurs 1a, 1b,...1n selon l'invention peuvent être montés en parallèle, chaque générateur recevant un signal d'horloge Clk délivré par un oscillateur 3' commun. Un tel ensemble de générateurs délivre à chaque cycle d'horloge Clk un nombre aléatoire ayant une longueur n correspondant au nombre de générateurs montés en parallèle. Les sorties respectives des générateurs peuvent être combinées d'une manière simple ou complexe dans un circuit logique 5'.

Le générateur représenté sur la figure 1 ou 7 est tout à fait adapté pour être intégré dans un

microcircuit tel que ceux qui équipent les cartes à puce, dont un exemple est représenté schématiquement en figure 6.

Le microcircuit 41 représenté comprend de façon classique une unité de traitement 42, par exemple un microprocesseur ou un microcontrôleur, des mémoires 44 de type ROM, RAM et/ou EEPROM, et un module de liaison 47 pour communiquer avec un terminal 51 externe, ces divers éléments étant interconnectés par un bus interne 43. Le microcircuit comprend également un générateur aléatoire 45 selon l'invention, incluant le générateur 1 précédemment décrit.

Le module de liaison 47, du type avec ou sans contact, est conçu pour coopérer avec un module de liaison 57 correspondant prévu dans un terminal 51, le terminal 51 comprenant lui-même une unité de traitement 52, des mémoires 54 et un bus interne 53 permettant à l'unité de traitement de communiquer avec les mémoires 54 et le module de liaison 57.

Le générateur aléatoire 45 intervient dans une procédure d'authentification du terminal 51 par le microcircuit 41, en vue d'autoriser une transaction.

A cet effet, l'unité de traitement 42 utilise le générateur 45 pour produire un nombre aléatoire "A" qui est transmis au terminal 51. Parallèlement, l'unité de traitement 42 calcule le résultat $R = F_{KS}(A)$ de la transformation du nombre aléatoire "A" par une fonction d'authentification F_{KS} à clé secrète KS. Le terminal 51, qui connaît la clé secrète KS, effectue le même calcul et transmet au microcircuit 41 le résultat R' de la transformation. Si le microcircuit constate que les deux résultats R et R' sont identiques, il accepte de procéder à la transaction demandée par le terminal.

De préférence, le terminal 41 comprend également un générateur aléatoire 55 selon l'invention pour authentifier le microcircuit. Dans ce cas, le terminal exécute une procédure analogue à celle qui vient d'être

décrite, en émettant un nombre aléatoire à destination du microcircuit, et en comparant le résultat calculé avec celui qui a été calculé et transmis par le microcircuit.

Il apparaîtra clairement à l'homme de l'art que le générateur aléatoire selon l'invention est susceptible de nombreux modes de réalisation, variantes et applications, tout en restant dans le cadre de l'enseignement qui précède.

REVENDICATIONS

1. Générateur de signal aléatoire du type utilisant une source de bruit électronique,

caractérisé en ce que la source de bruit électronique comprend un transistor MOS coudé présentant un courant drain-source ayant une composante aléatoire, le générateur comprenant des moyens pour produire un signal binaire aléatoire à partir de la composante aléatoire.

2. Générateur selon la revendication 1, dans lequel le transistor MOS coudé comprend un canal en forme de S ou en lacets dont les dimensions sont à la limite de la résolution offerte par la technique de fabrication du transistor.

3. Générateur selon l'une des revendications 1 et 2, comprenant un transistor de référence auquel sont appliqués une tension de grille et un courant de polarisation identiques à ceux appliqués au transistor coudé, pour extraire la composante aléatoire.

4. Générateur selon l'une des revendications 1 à 3, comprenant des moyens pour comparer la composante aléatoire à un courant de détection.

5. Générateur selon l'une des revendications 1 à 4, comprenant des moyens pour amplifier la composante aléatoire.

6. Générateur selon l'une des revendications 1 à 5, comprenant des moyens pour échantillonner le signal binaire aléatoire, de manière à obtenir un signal numérique aléatoire.

7. Générateur selon la revendication 6, comprenant un circuit logique (5) pour produire des nombres binaires aléatoires à partir du signal numérique aléatoire.

8. Générateur selon l'une des revendications 1 à 7, comprenant des moyens pour maintenir automatiquement la tension de grille (V_G) du transistor coudé dans une plage de valeurs déterminée assurant la délivrance d'un signal de sortie équiprobable.

9. Générateur selon l'une des revendications 1 à 8, comprenant plusieurs sources de bruit électronique produisant un courant ayant une composante aléatoire, chaque source étant couplée respectivement à des moyens pour générer un signal binaire aléatoire à partir de la composante aléatoire produite par la source, le générateur comprenant en outre des moyens pour combiner les signaux binaires aléatoires issus des sources pour produire des nombres binaires aléatoires.

10. Circuit intégré, caractérisé en ce qu'il comprend un générateur de signal binaire aléatoire selon l'une des revendications 1 à 9, et des moyens pour relier la sortie du générateur à d'autres composants du circuit intégré.

11. Circuit intégré selon la revendication 10, agencé sur un support pour former une carte à puce ou tout autre objet électronique portable équivalent.

12. Circuit intégré selon la revendication 10 ou 11, comprenant une unité de traitement comprenant des moyens pour recevoir un nombre aléatoire produit par le générateur, des moyens pour émettre ce nombre aléatoire à destination d'un terminal extérieur, des moyens pour appliquer à ce nombre aléatoire une fonction

d'authentification à clé secrète, des moyens pour comparer le résultat de cette fonction à un résultat fourni par le terminal en réponse à l'émission du nombre aléatoire, et des moyens pour autoriser une transaction avec le terminal si le résultat fourni par le terminal correspond au résultat calculé par l'unité de traitement.

13. Procédé pour générer un signal aléatoire à partir d'une source de bruit électronique, caractérisé en ce qu'il comprend les étapes consistant à :

- prévoir un transistor coudé présentant un canal en forme de S ou en lacets dont les dimensions sont choisies à la limite de la résolution offerte par la technique de fabrication du transistor,
- extraire une composante aléatoire de courant aux bornes d'un transistor MOS coudé,
- générer un signal binaire en fonction de la composante aléatoire, et
- échantillonner le signal binaire.

14. Procédé selon la revendication 13, comprenant des étapes consistant à amplifier la composante aléatoire et lui retrancher une valeur de référence avant de la convertir en un signal binaire.

15. Procédé selon l'une des revendications 13 et 14, comprenant une étape d'ajustement de la tension de grille du transistor coudé en fonction du signal binaire aléatoire obtenu à la suite de l'étape d'échantillonnage.

16. Procédé selon l'une des revendications 13 à 15, comprenant une étape consistant à générer des nombres binaires à partir du signal binaire.

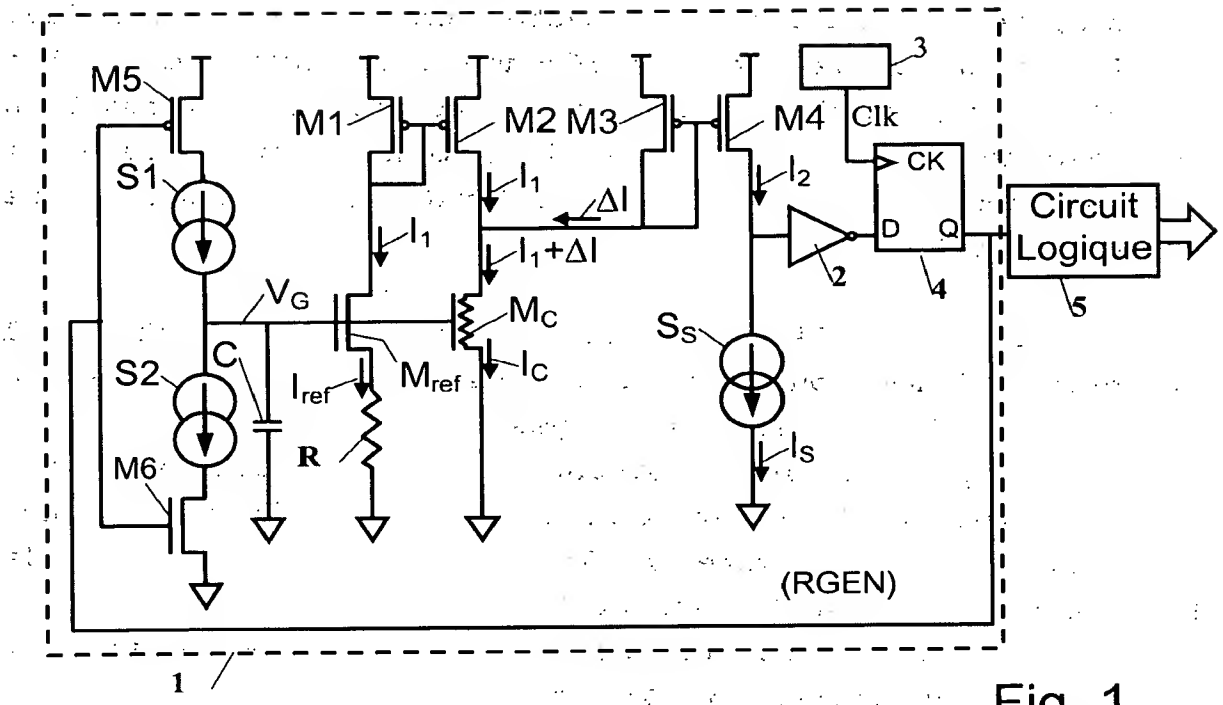

Fig. 1

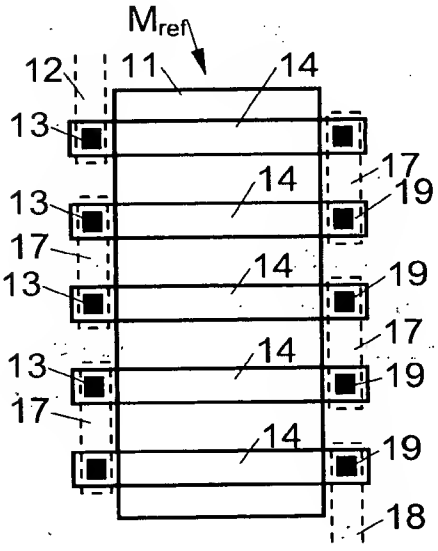

Fig. 2

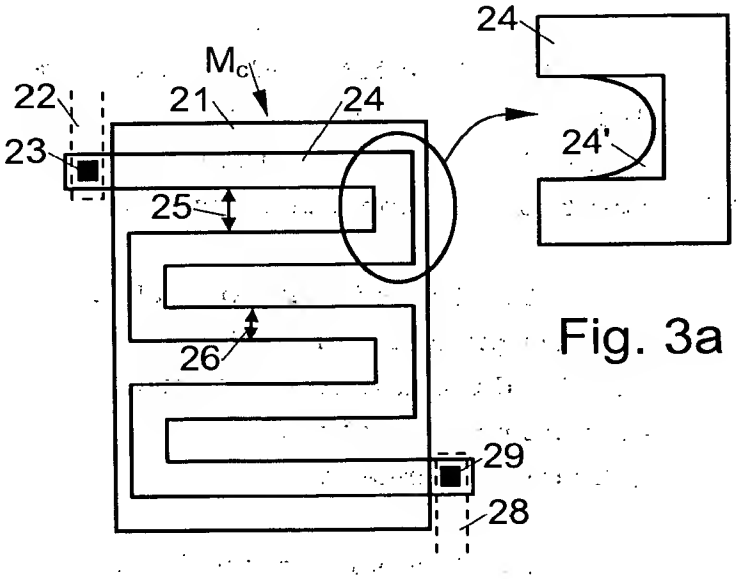

Fig. 3a

Fig. 3

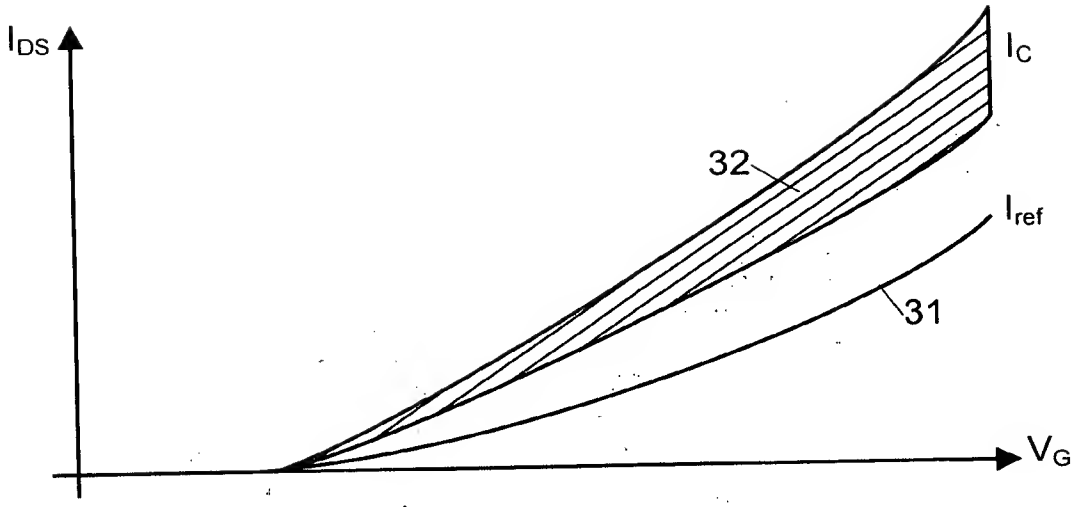

Fig. 4

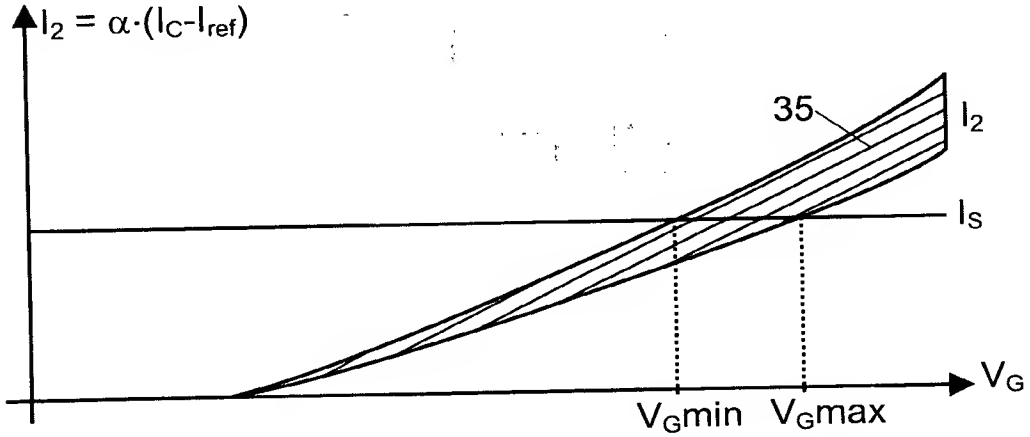

Fig. 5

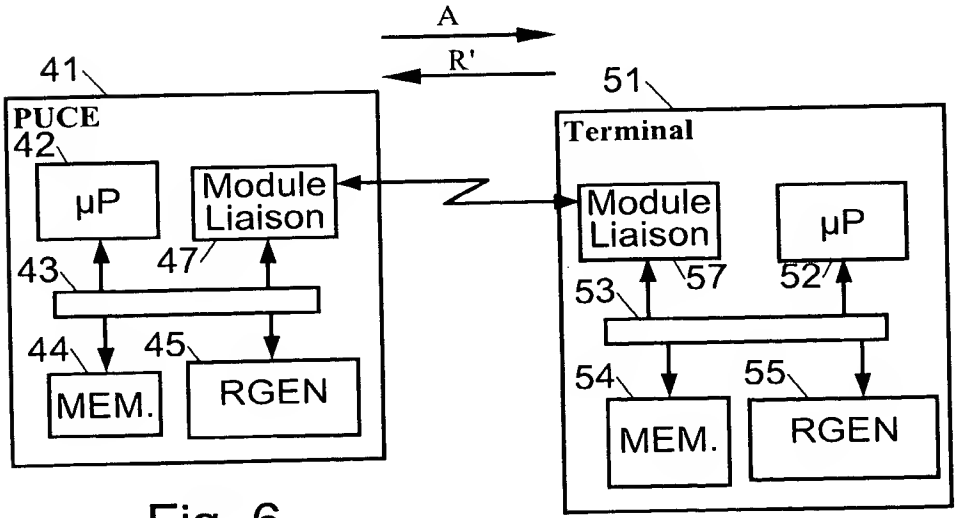

Fig. 6

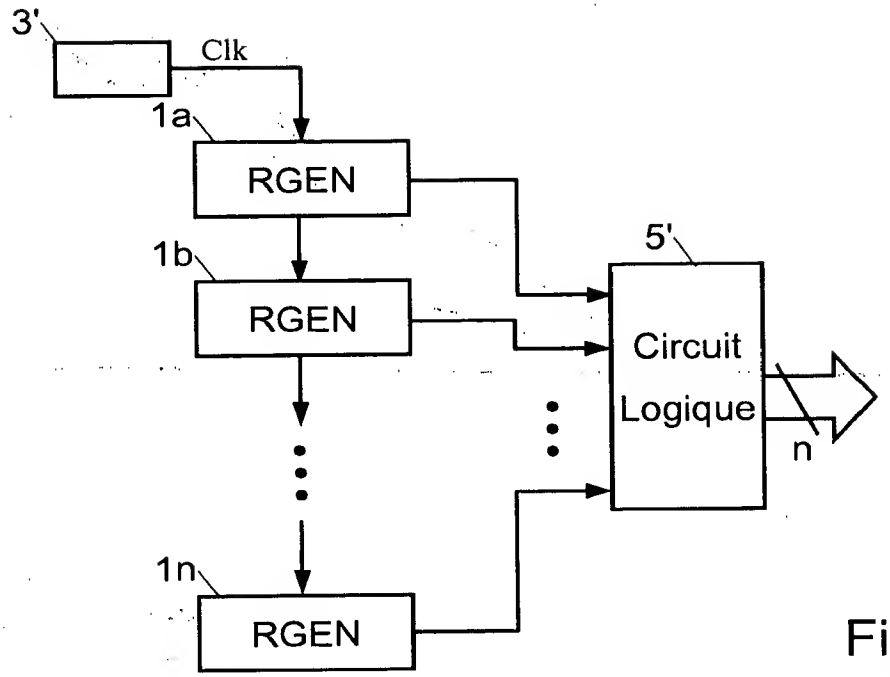

Fig. 7